事後評価報告書

１．研究課題名：

“Provably Secure Software Technology and Its Applications with the Special Focus on Smart Card and GRID Applications”

２．研究代表者名：

２－１．日本側研究代表者：慶應義塾大学　岡田　光弘

２－２．フランス側研究代表者：国立情報科学・制御研究所　Claude Kirchner

総合評価：　優

３．研究交流実施内容及び成果：

大規模な研究体制を組織し双方の多くの研究者が相互に訪問し情報交換等の交流が行われた。また、ワークショップやシンポジウムを日仏組織の共催によるもの、それぞれの組織の主催するものを数多く開催しており積極的に研究交流の機会が持たれた。その結果、それぞれの研究分野や研究手法について興味を共有する研究者ネットワークが構築できた。

日本側では、セキュリティ研究の中心目標として“provably secure”技術の具体的な研究が進められ、セキュリティプロトコルの安全性、型理論の安全性研究への応用、防災・環境・資源探索などでの観測グリッドにおける拡張性の大きいアクセス制御が可能な認証法、など多くの学術的成果が得られた。

仏国側では、セキュリティプロトコルの安全性検証法について新たな概念や手法、アクセス制御ポリシーの書き換えやプロトコル検証における新たなモデルや手法の研究において多くの学術的成果が得られた。

４．事後評価結果：

４－１．総合評価

実績のある多くの研究者が参加して、理論的な成果が数多く得られたと認められる。一方、申請時に提案された「provably secure なソフトウェア構築技術を開発する、確立する」という目標、あるいはその「応用への具体的な共同研究成果を提出する」ことは必ずしも達成されてない。これは目標設定が大きすぎたことにも原因がある。

また、CNRS 日仏共同研究拠点に情報セキュリティ部門が創設され、研究テーマを絞ってより集中度を高めた後続の共同研究プロジェクトが開始されているなど、今後の発展に期待できる。研究交流に関しては、これまでもある程度の実績があり、今回の事業によって今後の交流活発化の基盤を固め、持続的発展の可能性を広げたものと評価できる。

４－２．研究交流の有効性

大規模な研究体制を組織して、たくさんの成果が上がっている点、双方の多くの研究者が交流して、特定の研究分野や研究手法について興味を共有するネットワークが構築できた点が評価できる。研究テーマを絞ってより集中度を高めた後続の共同研究プロジェクトが開始されているなど、今後の発展に期待できる。また、フランス側から日本側への一方通行ではあるもののインターンシップ、研究者長期派遣などを通じて、人材育成への貢献が評価できる。

一方、相手国側研究チームとの共著論文発表が少ないことから、研究成果の多くはこのプロジェクトがなくてもそれぞれの研究者の努力で得ていたと考えられ、今回の日仏交流による新しい知の創造あるいは新分野の開拓の点における評価はしにくい。

４－３．当初目標の達成度

学術的成果として、目標としていたプロトコルの安全性・信頼性について論理面と形式面から同時に証明できる方法を新たに開発したこと、情報セキュリティ安全性研究について論理学やソフトウェア科学を応用する方法を開発したこと、など新しい成果が得られ、当初目標が達成されている。しかし、目標としていた次世代スマートカード開発に関する研究については、具体的にどのような成果が得られたのか読み取れなかった。

ワークショップの開催などについては、おおむね計画通りに進められ、研究者ネットワーク形成の目標を達成している。